

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT  
FÜR DEN PATENTWIRTSCHAFTSBEREICH

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>PHD 99.097W0</b>	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen <b>PCT/EP 99/07026</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>21/09/1999</b>	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>30/09/1998</b>
Anmelder <b>KONINKLIJKE PHILIPS ELECTRONICS N.V. et al.</b>		

Dieser Internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser Internationale Recherchenbericht umfaßt insgesamt 2 Blätter.



Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die Internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.



Die Internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die Internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das



in der internationalen Anmeldung in schriftlicher Form enthalten ist.



zusammen mit der internationalen Anmeldung in computerisierter Form eingereicht worden ist.



bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.



bei der Behörde nachträglich in computerisierter Form eingereicht worden ist.



Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.



Die Erklärung, daß die in computerisierter Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2.



**Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3.



**Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1



wie vom Anmelder vorgeschlagen



keine der Abb.



weil der Anmelder selbst keine Abbildung vorgeschlagen hat.



weil diese Abbildung die Erfindung besser kennzeichnet.

Best Available Copy

**THIS PAGE BLANK (USPTO)**

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 99/07026

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
 IPK 7 G07F7/10 G06F1/00 G06K19/073

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationsymbole)  
 IPK 7 G07F G06F G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	FR 2 745 924 A (CP8 TRANSAC) 12. September 1997 (1997-09-12) Zusammenfassung; Ansprüche 1,7-11,20; Abbildung 1	1-3
A	US 4 932 053 A (S. FRUHAUF) 5. Juni 1990 (1990-06-05) das ganze Dokument	1-3

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfindeterischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindeterischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

8. Februar 2000

Absendedatum des Internationalen Recherchenberichts

18/02/2000

Name und Postanschrift der Internationalen Recherchenbehörde  
 Europäisches Patentamt, P.B. 5618 Patentlaan 2  
 NL - 2280 HV Rijswijk  
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

David, J

# INTERNATIONALER RESEARCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 99/07026

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
FR 2745924	A	12-09-1997	AU	2031497 A	22-09-1997
			BR	9702118 A	26-01-1999
			CA	2221880 A	12-09-1997
			CN	1181823 A	13-05-1998
			EP	0826169 A	04-03-1998
			WO	9733217 A	12-09-1997
			JP	10507561 T	21-07-1998
			NO	975116 A	06-01-1998
			US	5944833 A	31-08-1999
US 4932053	A	05-06-1990	FR	2638869 A	11-05-1990
			EP	0368727 A	16-05-1990
			JP	2199561 A	07-08-1990
			JP	2813663 B	22-10-1998

## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 99/07026

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G07F7/10 G06F1/00 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F G06F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 745 924 A (CP8 TRANSAC) 12 September 1997 (1997-09-12) abstract; claims 1,7-11,20; figure 1	1-3
A	US 4 932 053 A (S. FRUHAUF) 5 June 1990 (1990-06-05) the whole document	1-3

☐ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

## \* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

8 February 2000

Date of mailing of the international search report

18/02/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3018

Authorized officer

David, J

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/EP 99/07026

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2745924 A	12-09-1997	AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		WO 9733217 A	12-09-1997
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998
		US 5944833 A	31-08-1999
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998


 INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation <sup>7</sup> : G07F 7/10, G06F 1/00, G06K 19/073		A1	(11) Internationale Veröffentlichungsnummer: WO 00/19386
			(43) Internationales Veröffentlichungsdatum: 6. April 2000 (06.04.00)

(21) Internationales Aktenzeichen: PCT/EP99/07026 (22) Internationales Anmeldedatum: 21. September 1999 (21.09.99)  (30) Prioritätsdaten: 198 44 992.5      30. September 1998 (30.09.98)    DE 199 36 939.9      5. August 1999 (05.08.99)      DE  (71) Anmelder (für alle Bestimmungsstaaten ausser US): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL). (71) Anmelder (nur für DE): PHILIPS CORPORATE INTELLECTUAL PROPERTY GMBH [DE/DE]; Habsburgerallee 11, D-52066 Aachen (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): FEUSER, Markus [DE/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). (74) Anwalt: PETERS, Carl, H.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).	(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  <b>Veröffentlicht</b> <i>Mit internationalem Recherchenbericht.</i> <i>Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>
---	--

(54) Title: DATA PROCESSING DEVICE AND METHOD FOR OPERATING SAME WHICH PREVENTS A DIFFERENTIAL CURRENT CONSUMPTION ANALYSIS

(54) Bezeichnung: DATENVERARBEITUNGSEINRICHTUNG UND VERFAHREN ZU DESSEN BETRIEB ZUM VERHINDERN EINER DIFFERENTIELLEN STROMVERBRAUCHANALYSE

(57) Abstract

The invention relates to a data processing device (100) and to a method for operating the data processing device, notably a chip card. Said device comprises an integrated circuit which in accordance with a clock pulse carries out calculating operations, especially cryptographic operations, data inputs and outputs and data transfers from and to registers of the integrated circuit. To this end the integrated circuit (10) is controlled such that the calculating operations, on the one hand, and the input/output of data and data transfer from register to register or between registers, on the other hand, are carried out time-parallel.

(57) Zusammenfassung

Die vorliegende Erfindung betrifft eine Datenverarbeitungseinrichtung (100) sowie ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte, mit einer integrierten Schaltung, welche in Abhängigkeit von einem Taktsignal Rechenoperationen, insbesondere kryptographische Operationen, Datenein- bzw. -ausgaben sowie eine Datenübergabe von bzw. zu Registern der integrierten Schaltung ausführt. Hierbei wird die integrierte Schaltung (10) derart gesteuert, dass das Ausführen von Rechenoperationen einerseits und die Datenein-/ausgabe sowie die Datenübergabe von Register zu Register bzw. zwischen Registern andererseits zeitlich parallel durchgeführt wird.

### LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidsschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland		Republik Mazedonien	TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von
CA	Kanada	IT	Italien	MX	Mexiko		Amerika
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun		Korea	PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		



Datenverarbeitungseinrichtung und Verfahren zu dessen Betrieb zum Verhindern einer differentiellen Stromverbrauchsanalyse.

Die Erfindung betrifft ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte, mit einer integrierten Schaltung, welche in Abhängigkeit von einem Taktsignal Rechenoperationen, insbesondere kryptographische Operationen, Datenein- bzw. -ausgaben sowie eine Datenübergabe zwischen Registern der integrierten Schaltung ausführt, gemäß dem Oberbegriff des Anspruchs 1. Die Erfindung betrifft ferner eine Datenverarbeitungseinrichtung, insbesondere Chipkarte, insbesondere zum Ausführen des Verfahrens, mit einer integrierten Schaltung, welche in Abhängigkeit von einem Taktsignal Rechenoperationen, insbesondere kryptographische Operationen, ausführt, wobei die integrierte Schaltung ein Rechenwerk mit zugeordnetem ersten Register und Datenein- und -ausgängen aufweist, gemäß dem Oberbegriff des Anspruchs 3.

In vielen Datenverarbeitungsgeräten mit integrierter Schaltung dienen beispielsweise kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät transportierten Daten. Die hierfür notwendigen Rechenoperationen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei in diesem Zusammenhang verwendeten Daten bzw. Zwischenergebnissen handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

Bei von der integrierten Schaltung durchgeführten Rechenoperationen, beispielsweise zur Berechnung von kryptographischen Algorithmen, werden logische Verknüpfungen zwischen Operanden bzw. Zwischenergebnissen durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden von leeren oder zuvor gelöschten Speicherbereichen bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert

einer Bit-Speicherzelle geändert wird, d.h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des in das leere Register  
5 geschriebenen Operanden (=Anzahl der Bits mit dem Wert "1") ansteigen. Durch eine entsprechende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise  
10 bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte  
15 Kryptoanalyse der kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann. Die "Differential Power Analysis" ermöglicht somit über eine reine Funktionalität hinaus zusätzliche interne Informationen einer integrierten Schaltung gewinnen zu können.

Aus der US 5 297 201 ist es bekannt, einen Hochfrequenz abstrahlenden  
20 Computer mit einer Einrichtung zu kombinieren, welche ebenfalls eine Hochfrequenz ähnlich zu derjenigen des Computers abstrahlt. Dadurch ist es für einen unberechtigten Dritten nicht mehr möglich, die Hochfrequenzabstrahlung des Computers zu dekodieren. Eine Kryptoanalyse durch einen Dritten, der unmittelbar Zugang zum Computer hat, kann dieses System jedoch nicht verhindern.

25 Die WO 90/15489 beschreibt ein gesichertes Kommunikationssystem, bei dem Dummyverkehr bzw. -übertragungen erzeugt werden, um kryptographische Analysen zu erschweren. Eine Kryptoanalyse durch einen Dritten, der unmittelbar Zugang zum Computer hat, kann dieses System jedoch ebenfalls nicht verhindert werden.

30 Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren und eine verbesserte Datenverarbeitungseinrichtung der obengenannten Art zur Verfügung zu stellen, welche die obengenannten Nachteile beseitigen und einen wirksamen Schutz gegen eine "Differential Power Analysis" zur Verfügung stellen.

Diese Aufgabe wird durch ein Verfahren der o.g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen und durch eine Datenverarbeitungseinrichtung der o.g. Art mit den in Anspruch 3 gekennzeichneten Merkmalen gelöst.

5 Dazu ist es bei dem Verfahren der o.g. Art erfindungsgemäß vorgesehen, dass die integrierte Schaltung derart gesteuert wird, dass das Ausführen von Rechenoperationen einerseits und die Datenein-/ausgabe sowie die Datenübergabe von Register zu Register bzw. zwischen Registern andererseits zeitlich parallel durchgeführt wird.

10 Dies hat den Vorteil, dass für eine "Differential Power Analysis" Anhaltspunkte dafür fehlen, wann eine Rechenoperation endet bzw. wann ein Auslesen/Beschreiben von Registern oder wann eine Datenein-/ausgabe erfolgt, da Zeitbereiche sowohl der eigentlichen Berechnungen als auch der Datenein- und Datenausgabe verschleiert werden. Die "Differential Power Analysis" wird somit erheblich erschwert, da von außen nicht mehr festgestellt werden kann, ob eine wirkliche Berechnung oder eine Ein-/Ausgabe stattfindet.

15 In einer vorteilhaften Weiterbildung des Verfahrens werden zum weiteren Verschleiern der Rechenoperationen sowie Datenein-/Ausgaben unmittelbar vor, während und/oder unmittelbar nach der Datenübergabe zwischen den Registern der integrierten Schaltung Dummyberechnungen von einem Rechenwerk der integrierten Schaltung ausgeführt, welche zufällige oder vorbestimmte Daten bearbeiten, wobei keine Daten in Register der integrierten Schaltung geschrieben werden.

20 Bei einer Datenverarbeitungseinrichtung der o.g. Art ist es erfindungsgemäß vorgesehen, dass ein mit dem ersten Register verbundenes zweites Register vorgesehen ist, welches die Datenein- und -ausgänge aufweist, wobei ferner eine Steuereinheit mit der integrierten Schaltung verbunden ist, welche derart ausgebildet ist, dass sie einen zeitlich parallelen Betrieb der Register zur Datenein-/ausgabe und Datenübergabe zwischen den  
25 Registern einerseits und Rechenoperationen der Recheneinheit andererseits steuert.

30 Dies hat den Vorteil, dass für eine "Differential Power Analysis" Anhaltspunkte dafür fehlen, wann eine Rechenoperation endet bzw. wann ein Auslesen/Beschreiben von Registern oder wann eine Datenein-/ausgabe erfolgt, da Zeitbereiche sowohl der eigentlichen Berechnungen als auch der Datenein- und Datenausgabe verschleiert werden. Durch das zweite Register ist eine Ein-/Ausgabe von Daten möglich, während das Rechenwerk aktiv ist und ggf. Daten in das erste Register schreibt oder Daten aus dem ersten Register ausliest. Die "Differential Power Analysis" wird somit erheblich erschwert, da von außen bei geeigneter Ansteuerung des zweiten Registers nicht mehr festgestellt werden kann, ob eine wirkliche Berechnung oder eine Ein-/Ausgabe stattfindet.

In einer vorteilhaften Weitergestaltungen der Datenverarbeitungseinrichtung ist das erste Register ein Operandenregister des Rechenwerkes und/oder das zweite Register ein Operandenregister der Datenein-/ausgabe.

5

Nachstehend wird die Erfindung anhand der beigelegten Zeichnungen näher erläutert. Diese zeigen in

Fig. 1 ein Blockschaltbild einer bevorzugten Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung,

10

Fig. 2 ein Blockschaltbild einer integrierten Schaltung der Datenverarbeitungseinrichtung von Fig. 1,

Fig. 3 eine graphische Veranschaulichung der Aktivität der erfindungsgemäßen Datenverarbeitungseinrichtung über die Zeit gemäß dem Stand der Technik und

15

Fig. 4 eine graphische Veranschaulichung der Aktivität der erfindungsgemäßen Datenverarbeitungseinrichtung über die Zeit gemäß der Erfindung.

Fig. 1 zeigt eine bevorzugte Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung 100 mit einer integrierten Schaltung 10, einem Register 12 mit Programmzugriff 14 und einer Steuereinheit 16. Über Leitung 18 erhält die Steuereinheit 16 sowie die integrierte Schaltung ein in Fig. 3 und 4 dargestelltes Taktsignal 20. Über Steuerleitungen 22 steuert die Steuereinheit 16 die integrierte Schaltung 10, die Dateneingänge 24 und Datenausgänge 26 aufweist.

25

Wie aus Fig. 2 ersichtlich ist umfasst die integrierte Schaltung 10 ein Rechenwerk 28, ein dem Rechenwerk 28 zugeordnetes erstes Operandenregister 30 und ein mit dem ersten Operandenregister 30 verbundenes zweites Operandenregister 32. Die Dateneingänge 24 und Datenausgänge 26 sind am zweiten Operandenregister 32 angeordnet. Das Taktsignal 20 (Fig. 3 und 4) wird über die Leitung 18 sowohl an das Rechenwerk 28 als auch an die beiden Operandenregister 30 und 32 weitergeleitet. Bei Ausführung von Berechnungen bzw. Operationen durch das Rechenwerk 28 liest dieses aus dem ersten Register 30 Daten aus bzw. schreibt ein Ergebnis einer Berechnung in das erste Register 30 ein. Zwischen den Registern 30 und 32 erfolgt ein entsprechender Datenaustausch bzw. eine gegenseitige Datenübergabe, nachfolgend als R2-1 bezeichnet, wenn Daten von dem zweiten

30

Register 32 an das erste Register 30 übergeben werden, bzw. als R1-2 bezeichnet, wenn Daten von dem ersten Register 30 an das zweite Register 32 übergeben werden. Eine der von der Steuereinheit 16 kommenden Steuerleitung 22 ist mit dem zweiten Register 32 zu dessen Steuerung verbunden, während eine andere Steuerleitung 22 mit dem ersten Register 30 zu dessen Steuerung verbunden ist.

Eine von Paul Kocher im Internet unter <http://www.cryptography.com/dpa> veröffentlichte "Differential Power Analysis" hat den Ansatz, dass neben den Ein/Ausgangssignalen zusätzlich eine Stromaufnahme  $I_a$  bzw. Spannungseinbrüche  $\Delta U_a$  einer Versorgungsspannung  $U_a$  der integrierten Schaltung analysiert werden. Der Erfolg dieser Analysemethode hängt davon ab, ob man eine Anzahl  $N_A$  von analogen ( $I_a(t)$  oder  $\Delta U_a(t)$ ) Signalverläufen  $S(k,t)$  über die Zeit mit  $k=\{1,...,N_A\}$  unterschiedlichen Operanden derart aufnehmen kann, dass eine Summenbildung der Form

$$T(i,t) = \sum_{k=1}^{N_A} p(i,k) \cdot S(k,t)$$

mit den Koeffizienten  $p(i,k)$  mit  $i=\{0,1,2,...\}$  möglich ist. Betrachtet man unterschiedliche Signalverläufe  $S(k_1,t_1)$ ,  $S(k_2,t_1)$ ,  $S(k_3,t_1)$ ... zum gleichen Zeitpunkt  $t=t_1$ , kann eine "Differential Power Analysis" nur funktionieren, wenn die integrierte Schaltung in diesem Moment die gleiche Rechenoperation mit unterschiedlichen Operanden  $k=\{1,...,N_A\}$  ausführt, d.h. die Signalverläufe  $S(k,t)$  müssen genau übereinandergelegt werden können. Dieses gilt nicht nur für die Berechnung selbst, sondern auch für die Ein- und Ausgabe von Daten.

Die Erfindung verschleiert sowohl die Zeitbereiche, der eigentlichen Berechnung als auch die Zeitbereiche der Datenein- bzw. Datenausgabe. Bei geeigneter Ansteuerung des zweiten Registers 32 kann von außen nicht mehr festgestellt werden, wann eine wirkliche Berechnung oder eine Ein-/Ausgabe stattfindet. Die "Differential Power Analysis" wird somit erheblich erschwert. Die integrierte Schaltung 10 ist erfindungsgemäß mit den beiden Operandenregistern 30 und 32 ausgestattet. Diese erlauben eine Ein- und Ausgabe von Daten über das zweite Operandenregister 32 mit dessen Dateneingängen 24 und Datenausgängen 26 auch während das Rechenwerk 28 unter Nutzung des ersten Operandenregisters 30 aktiv ist und Berechnungen bzw. Operationen ausführt.

Fig. 4 veranschaulicht eine Betriebsweise der erfindungsgemäßen Datenverarbeitungseinrichtung 100, wobei über eine Zeitachse 34 das Taktsignal 20 und ein Betriebszustand von Rechenwerk bzw. Operandenregistern angegeben ist. Hierbei bezeichnet

36 einen Betriebszustand, bei dem das Rechenwerk eine Berechnung ausführt. Mit 38 ist ein Betriebszustand bezeichnet, bei dem eine Datenein- bzw. Datenausgabe stattfindet, mit 40 ist ein Betriebszustand bezeichnet, bei dem eine Datenübergabe R1-2 stattfindet und mit 42 ist ein Betriebszustand bezeichnet, bei dem eine Datenübergabe R2-1 stattfindet.

5                    Fig. 3 veranschaulicht in einer zu Fig. 3 analogen Darstellung zum Vergleich eine Betriebsweise einer herkömmlichen Datenverarbeitungseinrichtung. Hier sind die Ein- bzw. Ausgabephasen 38 der eigentlichen Berechnung 36 zeitlich vor- bzw. nachgeschaltet. Bei der "Differential Power Analysis" können die Phasen der Berechnungen 36 und der Ein-/Ausgabe 38 leicht identifiziert werden, insbesondere welche Eingaben 38 bei einer Berechnung 40 Verwendung finden und welche Ausgaben 38 die Folge sind.

10                    Bei der in Fig. 4 dargestellten, erfindungsgemäßen Betriebsweise werden mittels der Steuereinheit 16 die Berechnungen 36 sowie die Datenein-/ausgaben 38, 40, 42 dadurch verschleiert, dass der Datenfluss der beiden Operandenregister 30, 32 zeitlich parallel zu den Berechnungen 36 gesteuert wird. Berechnungen 36 finden immer statt. Ob aber eine  
15 Berechnung 40 von der Eingabe 38 abhängt oder eine Ausgabe 38 liefert, wird durch die Kopieraktionen R1-2 40 und R2-1 42 bestimmt. Die Berechnungen vor R2-1 42 bzw. nach R1-2 40 sind beispielsweise Dummyberechnungen. Dummyrechenoperationen sind solche Rechenoperationen, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis verworfen wird und nicht in die Ergebnisse bzw. Eingangsdaten der  
20 wirklichen Rechenoperationen eingehen. Zusätzliche Dummyein-/ausgaben sind ferner optional vorgesehen. Sowohl die Dummyberechnungen als auch die Dummyeingaben/Dummyausgaben erzeugen Strom- bzw. Spannungsänderungen, welche denen der wirklichen Berechnungen und Ein-/Ausgaben sehr ähnlich sind.

25                    Die erfindungsgemäß zum Schutz der integrierten Schaltungsteile 10 gegen "Differential Power Analysis" vorgesehene Steuereinheit 16 zielt speziell auf die Ein-/Ausgabephasen 38, 40, 42 einer in den integrierten Schaltungsteilen 10 mit Hilfe digitaler, elektronischer Signalverarbeitung durchzuführenden Berechnungen 36 ab, da auch Ein-/Ausgaben anhand des Stromverbrauches mittels der "Differential Power Analysis" analysiert werden könnten. Entsprechend ist bei der "Differential Power Analysis" von Interesse, wann  
30 eine Berechnung 36 beginnt oder endet. Genau diese Informationen werden von dem erfindungsgemäßen Verfahren bzw. bei der erfindungsgemäßen Vorrichtung im Stromverbrauchssignal unterdrückt

## BEZUGSZEICHNENLISTE:

	100	Datenverarbeitungseinrichtung
	10	integrierte Schaltung
	12	Register
	14	Programmzugriff
5	16	Steuereinheit
	18	Leitung
	20	Taktsignal
	22	Steuerleitungen
	24	Dateneingänge
10	26	Datenausgänge
	28	Rechenwerk
	30	erstes Operandenregister: R1
	32	zweites Operandenregister R2
	34	Zeitachse
15	36	Berechnung
	38	Datenein- bzw. Datenausgabe
	40	Datenübergabe R1-2
	42	Datenübergabe R2-1

## PATENTANSPRÜCHE:

1. Verfahren zum Betreiben einer Datenverarbeitungseinrichtung (100), insbesondere einer Chipkarte, mit einer integrierten Schaltung (10), welche in Abhängigkeit von einem Taktsignal Rechenoperationen, insbesondere kryptographische Operationen, Datenein- bzw. -ausgaben (38) sowie eine Datenübergabe (40) von bzw. zu Registern der  
5 integrierten Schaltung (10) ausführt, dadurch gekennzeichnet, dass die integrierte Schaltung (10) derart gesteuert wird, dass das Ausführen von Rechenoperationen einerseits und die Datenein-/-ausgabe (38) sowie die Datenübergabe (40) von Register zu Register bzw. zwischen Registern (30,32) andererseits zeitlich parallel  
10 durchgeführt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass unmittelbar vor, während und/oder unmittelbar nach der Datenübergabe von Register zu  
15 Register bzw. zwischen den Registern (30, 32) der integrierten Schaltung Dummyberechnungen von einem Rechenwerk (28) der integrierten Schaltung (10) ausgeführt werden, welche zufällige oder vorbestimmte Daten bearbeiten, wobei keine Daten in Register (30, 32) der integrierten Schaltung geschrieben werden.
- 20 3. Datenverarbeitungseinrichtung (100), insbesondere Chipkarte, insbesondere zum Ausführen eines Verfahrens gemäß wenigstens einem der vorhergehenden Ansprüche, mit einer integrierten Schaltung (10), welche in Abhängigkeit von einem Taktsignal (20) Rechenoperationen, insbesondere kryptographische Operationen, ausführt, wobei die integrierte Schaltung (10) ein Rechenwerk (28) mit zugeordnetem ersten Register (30) und  
25 Datenein- und -ausgänge (24, 26) aufweist, dadurch gekennzeichnet, dass ein mit dem ersten Register (30) verbundenes zweites Register (32) vorgesehen ist, welches die Datenein- und -ausgänge (24, 26) aufweist, wobei ferner eine Steuereinheit (16) mit der integrierten Schaltung (10) verbunden ist, welche derart ausgebildet ist, dass sie einen zeitlich



parallelen Betrieb der Register (30, 32) zur Datenein-/ausgabe (38) und Datenübergabe (40) von Register zu Register bzw. zwischen den Registern (30, 32) einerseits und Rechenoperationen (40) der Recheneinheit (28) andererseits steuert.

- 5 4. Datenverarbeitungseinrichtung (100) nach Anspruch 3, dadurch gekennzeichnet, dass das erste Register (30) ein Operandenregister des Rechenwerkes (28) und/oder das zweite Register (32) ein Operandenregister der Datenein-/ausgabe (38) ist.

**THIS PAGE BLANK (USPTO)**

Fig.1 1/1

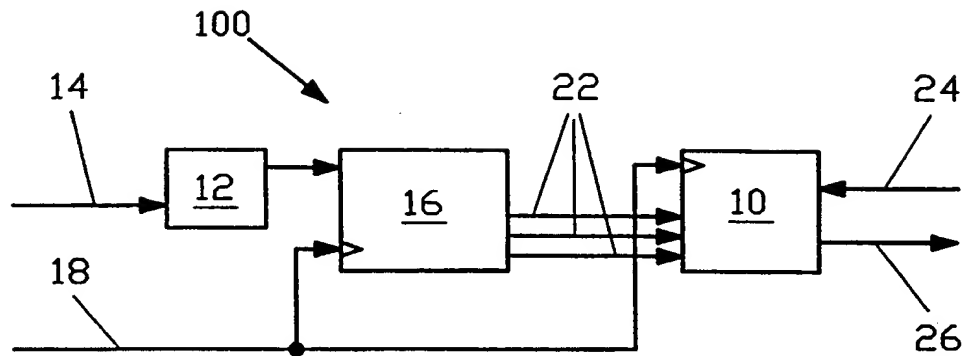


Fig.2

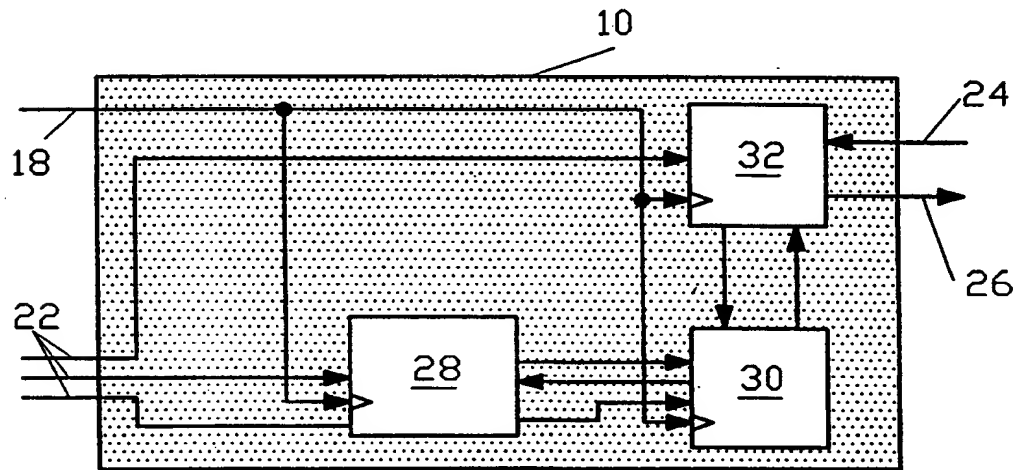


Fig.3

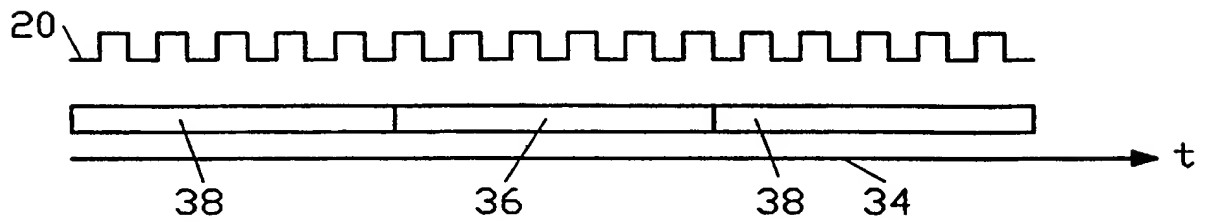
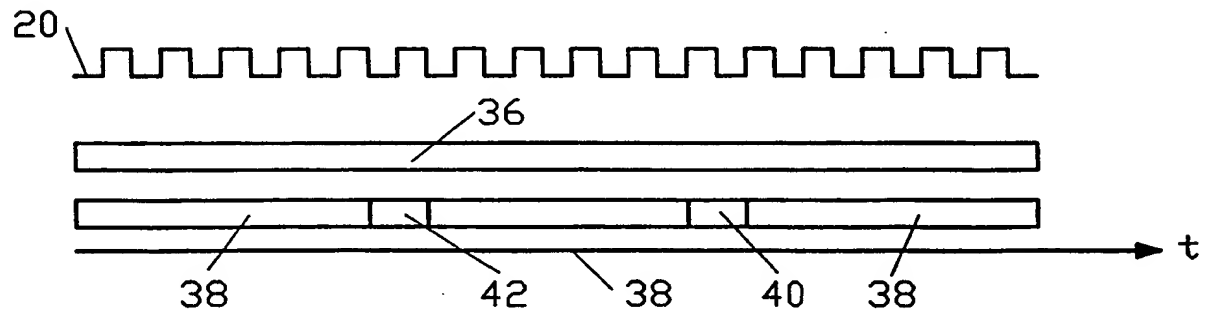


Fig.4



**THIS PAGE BLANK (0010)**

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: \_\_\_\_\_**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**